InfoCage®/モバイル防御

インストールガイド

日本電気株式会社, NEC システムテクノロジー株式会社

目　次

第1章 はじめに

　このたびは、InfoCage/モバイル防御をお買い上げいただき、まことにありがとうございます。
　InfoCage/モバイル防御（以下「本ソフトウェア」という）は、パソコンからの情報漏洩を防止するため、認証を受けていない人がそのパソコンを使うことを防止したり、データを暗号化して読めないようにしたりすることができる情報漏洩対策セキュリティソフトウェアです。

　本ソフトウェアには、メディア鍵で認証する「メディア鍵認証方式」と、パスワードで認証する「パスワード認証方式」があります。

※「メディア鍵認証方式」と「パスワード認証方式」の併用はできません。インストール時に選択してください。

　本ソフトウェアで情報漏洩を防止するためには、インストール時にパソコンを使用する人を認証する「鍵」の作成または、「パスワード」の設定を行い、その後保護が必要なファイルの暗号化を行う必要があります。
本インストールガイドに従ってそれぞれ設定を行ってください。

インストール後はパソコンを再起動する必要があります。他のプログラムを実行中の場合は、終了させてください。

※　本インストールガイドに記載されている「MobileProtect」（プログラムでの表示）と「InfoCage/モバイル防御」は同一製品です。

≪ 商標・著作権について ≫

- Microsoft および Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- VMware　は米国VMware, Inc.の商標です。
- Virtual　PC　は米国Connectix社の商標です。
- StandbyDisk、StandbyDisk Solo、およびStandbyDisk Solo RBは、StandbySoft LLC　／　(株)ネットジャパンの商標です。
- FINALDATA　は、FINALDATA INC.またはAOSテクノロジーズ株式会社の登録商標です。
- V2i Protector　はPowerQuest Corporationの商標です。
- DirectCD　および　Easy CD Creator　は、Adaptec社の商標です。
- B's CliP　および　B'sRecorder Gold　は、株式会社ビー・エイチ・エーの登録商標です。
- RecordNow!　はSonic Solutions社の登録商標です。
- Norton SystemWorks　は　Symantec Corporation　の商標です。
- ThumbDrive　はTrek 2000 International Ltd.のシンガポールおよびその他の国における登録商標です。
- Swipe　はティアック株式会社の商標です。
- InfoCage　は日本電気株式会社の登録商標です。
- MobileProtect　はＮＥＣシステムテクノロジー株式会社の登録商標です。
- その他、本マニュアルに記載されている会社名、商品名は各社の商標または登録商標です。
- このマニュアルの一部、又は全部を流用・複写することはできません。

本ソフトウェアの特徴

◆　メディア鍵認証方式

■パソコンのロック

鍵を格納したリムーバブルメディア等をパソコンから抜くことでパソコンをロックし、操作ができないようにすることができます。また、鍵を装着することでロックを解除できます。

パソコンのロック機能のみでは情報漏洩対策は万全ではありません。重要なファイルは必ず暗号化してください。

■ファイルの暗号化

ドライブ、フォルダ単位でデータの暗号化を行い、鍵となるリムーバブルメディアが装着された場合のみファイルアクセスが可能になります。
パソコン内のデータだけでなく、リムーバブルメディア内のデータも暗号化できます。

■データの抜き取り防止

認証されていないリムーバブルメディアへのコピーを禁止して、情報の抜き取りを防止します。

●　「鍵」とは

例えば鍵がなければドアが開かないのと同様に、リムーバブルメディアの「鍵」がなければパソコンの情報にアクセスできないようにするものです。

●　「鍵情報」とは

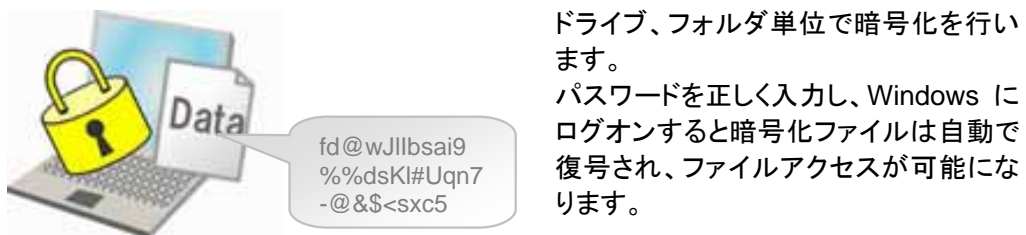
各メディアに作成した「鍵」のバックアップデータを「鍵情報」といい、「鍵」となるメディアとは別のリムーバブルメディアまたはネットワークの共有フォルダに保存しておきます。
「鍵」を保存したリムーバブルメディア内のデータを紛失した場合は、「鍵情報」を元に復旧します。

◆　パスワード認証方式

■パソコンのロック

本ソフトウェアのパスワードが正しく入力された場合のみ、Windows にログオンすることが可能になります。

■ファイルの暗号化

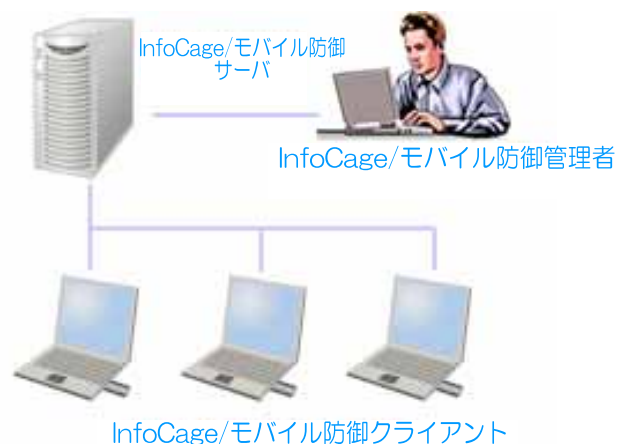
ドライブ、フォルダ単位で暗号化を行います。
パスワードを正しく入力し、Windows にログオンすると暗号化ファイルは自動で復号され、ファイルアクセスが可能になります。

● セキュリティチップ（TPM）でのセキュリティ強化

セキュリティチップ（TPM）搭載のパソコンをお使いの場合、セキュリティチップ（TPM）が有効となっている場合により強固なセキュリティを実現します。

スタンドアローンモードとネットワークモード

本ソフトウェアでは、クライアントパソコン単体で運用するスタンドアローンモードと、InfoCage/モバイル防御 管理サーバがクライアントの設定などを管理するネットワークモードがあります。
インストール時に運用方法を選択する必要がありますので、本ソフトウェアの管理者に確認後インストールを実施してください。

＜スタンドアローンモード＞
・メディア鍵認証方式
・パスワード認証方式

＜ネットワークモード＞
・メディア鍵認証方式
・パスワード認証方式

第2章 インストールの前にお読みください

2.1　注意事項

● 初期暗号化モードの設定
本ソフトウェアは、下記の 2 通りのモードでインストールを行うことができます。

・ ドライブ一括暗号モード（既定の導入モード）
本ソフトウェアが推奨する設定でインストールを行います。本モードでインストールを行う場合は、初期暗号化モードの設定は不要です。

・ 個別暗号モード
暗号化するドライブやフォルダを個別に指定して運用するときは、個別暗号モード用のインストールモジュールを作成してインストールを行います。

※ 初期暗号化モードを設定せずにインストールを行うと、「ドライブ一括暗号モード」でインストールされます。
※ 初期暗号化モードの設定は、「第 7 章　初期暗号化モードの設定」を参照してください。

※以降の注意事項は、ドライブ一括暗号モードと個別暗号モードで共通です。

● お願い

・ インストールおよびアップグレードインストールを行う前に、P.7の「導入前の注意確認事項」チェックシートを使用して、インストール環境の確認を行ってください。

・ 万が一に備え、大切なデータはバックアップを取ってから使用してください。

● サポート対象オペレーティングシステム

・Windows　XP　Professional（日本語版）　/　Home Edition（日本語版）
・Windows　2000　Professional（日本語版）
※ Microsoft 社から提供される最新パッチや ServicePack の適用をお奨めします。

1.　インストール

- 他の暗号化ソフトと併用すると、正しく動作しない場合があります。
※ InfoCage/ファイル暗号とは併用が可能であることを確認しています。
- 常駐しているプログラムがある場合は、暗号化を実行する前に終了してください。
※ 終了させずに暗号化を実行した場合、これらのファイルは暗号化されません。
- アドミニストレータ権限のあるユーザでインストールを行ってください。
【MobileProtect ユーティリティ】の操作もコンピュータの管理者（アドミニストレータ権限）で行ってください。また、Windows XP の「別のユーザとして実行」機能は使用しないでください。
- プロダクト ID はユーザ証書に記載されています。
- インストール時に入力するスーパーバイザパスワード／ユーザパスワードは、【MobileProtect ユーティリティ】起動時、鍵の復旧時、アンインストール時に必要になりますので、絶対に忘れないように注意してください。
- 本ソフトウェアを正常にインストールした後に、同じバージョンの setup.exe を実行するとアンインストールのウィザードが起動しますのでご注意ください。
- NTFS ファイルシステムの暗号化、または圧縮されたファイルは本ソフトウェアでは暗号化できないため、NTFS ファイルシステムの暗号化、または圧縮している場合は、本ソフトウェアをインストールする前に解除してください。
- SUBST コマンドを使用して仮想ドライブを割り当てている場合、本ソフトウェアをインストールする前に解除してだい。

- Windows XPに本ソフトウェアをインストールすると、OS標準のバックアップ機能が使用できなくなります。
  バックアップをおこなう場合は、本ソフトウェアのインストールフォルダ（通常は ¥Program Files¥MobileProtect ）内の ¥tools¥MPBackup.exe を使用してバックアップをおこなってください。操作方法については、同じフォルダ内の バックアップツール.pdf を参照してください。
- 本ソフトウェアをインストールすると、OS標準の「システムの復元」が使用できなくなります。
- Windows XP に本ソフトウェアをインストールすると、ユーザ選択画面が表示されなくなり、「簡易ユーザ切り替え」ができなくなります。
  また、シャットダウン時の画面が「コンピュータの電源を切る」（ボタン選択）画面から、「Windowsのシャットダウン」（プルダウンメニュー選択）画面に変更されます。
- 本ソフトウェアをインストールすると「Windows へようこそ」画面が通常のログオン画面に変更されます。
  ※Windowsの設定によっては、「Windows へようこそ」画面は表示されません。
- 本ソフトウェアをインストール後は、コントロールパネル等からユーザのログオンやログオフの方法を変更することができなくなります。セキュリティ強化のため、「Ctrl+Alt+Del」キーを押下する画面を表示するように設定を変更する場合は、インストール前に設定変更してください。

2. 暗号化について

- NTFSファイルシステムの場合、暗号化するファイルとフォルダは、SYSTEMアカウントの変更権限が必要です。

＜変更方法＞
（Windows XP Professional および Windows 2000 Professional のみ変更可能です。）
1. SYSTEMアカウントを変更したいフォルダを右クリックし、表示されるメニューの中から「プロパティ」をクリックしてください。
2. 「セキュリティ」タブを選択してください。
3. 「グループ名またはユーザ名」から「SYSTEM」を選択し、「アクセス許可」の「フルコントロール」の「許可」にチェックを入れ、「OK」をクリックしてください。

- NTFSファイルシステムの暗号化または圧縮されたファイルは暗号化できません。
- 暗号化指定したフォルダを共有設定しないでください。
- 暗号化したリムーバブルメディアおよびハードディスクドライブを本バージョンの InfoCage/モバイル防御がインストールされているパソコンに装着した場合、一部のファイルが正常に読み込みできないことがあります。

3. アップグレードインストールの注意事項

- 暗号化した外付けハードディスクドライブおよびリムーバブルディスクがある場合は、必ずパソコンに装着した状態でアップグレードインストールを行ってください。パソコンから取り外した状態でアップグレードした場合、一部のファイルが正常に読み込みできないことがあります。

4. メディア鍵認証方式の注意事項

(1) 事前にご準備いただくもの
インストールにはリムーバブルメディアが2個必要です。
使用にあたっては、鍵を格納するリムーバブルメディア(*1)と、鍵情報を格納するためのリムーバブルメディア(*2)が必要ですので、インストールする前に準備しておいてください。

*1：USBメモリ、フラッシュメモリカード、モバイルディスクの他、サーバの共有フォルダが使用できます。
（推奨：USBメモリ）
*2：フロッピーディスク、USBメモリ、フラッシュメモリカード、モバイルディスクが使用できます。
ただし、別売の「InfoCage/モバイル防御管理サーバ」と連携して動作するネットワークモードで使用する場合は、鍵情報はサーバに保存されますので、鍵情報を格納するメディアは必要ありません。

(2) 注意事項

- 鍵情報の保存
  スタンドアローン運用時、鍵情報は鍵を作成したメディアには保存できません。

- 鍵について
  本ソフトウェアで保護されたパソコンを使用する際には、必ず鍵を作成したメディアを装着した状態で使用してください。
  鍵を装着しない状態で使用した場合は、データが不正になる場合があります。
  また、鍵を装着していない場合、ごみ箱へのファイル削除が拒否されます。

5. アプリケーション競合問題について

次のアプリケーションソフトは、本ソフトウェアと同時に利用、または本ソフトウェアがインストールされた環境で利用すると、問題が発生することがあります。
これらのアプリケーションソフトは本ソフトウェアをインストールする前にアンインストールしておいてください。アンインストールできない場合は使用しないでください。

本ソフトウェアと共存できないアプリケーション

- 他のファイル暗号化ソフト、独自のログオン認証を行うソフト
- 仮想マシン環境構築ソフト（VMware、VirtualPC など）
- データバックアップ、リカバリソフト（StandbyDisk、StandbyDisk Solo、StandbyDisk Solo RB、FINALDATA など）
- 一部のディスクイメージ（HDD バックアップ）作成ソフト（V2i Protector など）
- Trek 社サムドライブ Touch G3/ティアック株式会社 Swipe FINGERPRINT USB メモリ、NEC 製ノートパソコン内蔵の指紋センサ以外を使用する指紋認証システム
  （NEC 製ノートパソコンに内蔵されている指紋センサを使用した認証システムと、本ソフトウェアの認証システムとの併用が可能です。ただし、上記の指紋認証システムのように連携させることはできません）
- 一部のライティングソフト（B'sCLiP など）
- Norton SystemWorks（Norton Utilities）の Norton Protection（ごみ箱機能）は使用できません。使用している場合は本ソフトウェアをインストールする前に解除してください。

＜解除方法＞
1.デスクトップの「Norton ごみ箱」のアイコンを右クリックし、[プロパティ]をクリックしてください。
2.[Norton Protection]タブを選択してください。
3.プルダウンメニュー[ドライブ]で、ドライブを選択し、[保護を有効にする]チェックを外してください。
※必ず全ドライブ無効にしてください。
4.[OK]をクリックしてください。

※ 設定を変更しない場合、ファイルの暗号化や復号に失敗する可能性があります。

使用に制限のあるアプリケーション

- 一部のライティングソフト（Windows XP 標準 CD 書き込み機能、DirectCD など）で CD-R/RW などにファイルを書き込みする場合は、暗号化されていないフォルダにファイルをコピーもしくは移動した後に操作を行ってください。

※ 下記のライティングソフトは本ソフトウェアとは併用が可能であることを確認しています。
  - RecordNow
  - B'sRecorder Gold
  - Easy CD Creator

【導入前の注意確認事項】チェックシート

氏名＿＿＿＿＿＿＿＿＿＿＿＿

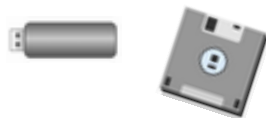
<table>
<tr><th rowspan="2"></th><th rowspan="2">確　認　事　項</th><th colspan="2">チェック欄</th></tr>
<tr><th>メディア鍵
認証方式</th><th>パスワード
認証方式</th></tr>
<tr><td>1</td><td>重要なデータは、念のためバックアップを取ること。</td><td></td><td></td></tr>
<tr><td>2</td><td>合鍵用のメディア、あるいはサーバを用意すること。</td><td></td><td>／</td></tr>
<tr><td>3</td><td>充分な空き容量が各ドライブにあること。

※暗号化を実行する際、テンポラリ（一時作業スペース）として以下の空き容量がドライブ毎に必要になります。
必要な空き容量　＝　暗号化対象ファイルの中で最大のファイルと同等の容量　＋（ドライブ容量×0.02）
（上記は最低限必要な容量です。暗号化処理は、十分な空き容量がある状態で行ってください。）

※ただし、初めて暗号化処理を行う場合は全てのドライブのごみ箱を暗号化するため、暗号化指定していないドライブにも上記の空き容量が必要となりますのでご注意ください。</td><td></td><td></td></tr>
<tr><td>4</td><td>フォルダ名やファイル名に日本語、または英語以外の文字列を使用している場合は、日本語、または英語に変更すること。</td><td></td><td></td></tr>
<tr><td>5</td><td>共存不可のアプリケーションの確認・対策を行うこと（「アプリケーション競合問題について」を参照。</td><td></td><td></td></tr>
<tr><td>6</td><td>暗号化するフォルダやファイルに SYSTEM 変更権限があることを確認すること。</td><td></td><td></td></tr>
<tr><td>7</td><td>デュアルブートマシンでないこと。</td><td></td><td></td></tr>
<tr><td>8</td><td>仮想ドライブを割り当てていないこと。</td><td></td><td></td></tr>
</table>

※このシートをコピーして使用してください。

2.2　クライアントのパソコンへの導入の流れ

1．リムーバブルメディアを用意（メディア鍵認証方式のみ）

鍵や鍵情報を保存するリムーバブルメディアを用意

2．インストール

・運用形態の選択
・スーパーバイザパスワード／ユーザパスワードの設定
・インストール

3．暗号化ウィザード

＜メディア鍵認証方式＞

①パソコンの鍵を作成　②鍵情報の保存　③暗号化

＜パスワード認証方式＞

暗号化

4．終　了

運用形態等が管理者によってあらかじめ設定されている場合は、本ガイドの操作手順と異なる場合があります。

第3章　InfoCage/モバイル防御のインストール

3.1　インストール（Step1）

注意

インストールおよびアップグレードインストールを行う前に、本ソフトウェアを使用する環境をチェックしてください。

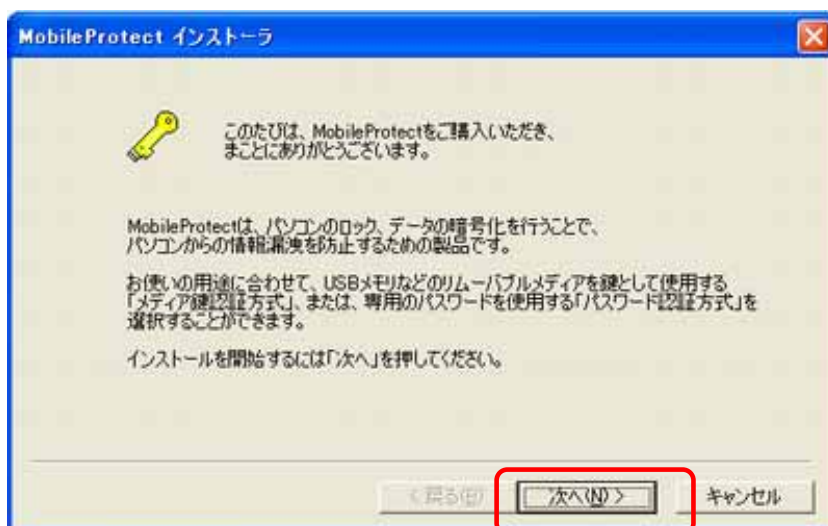
（環境のチェック方法）

本ソフトウェアが格納されているメディア（例　CD-ROM）内の下記のファイルを実行してください。

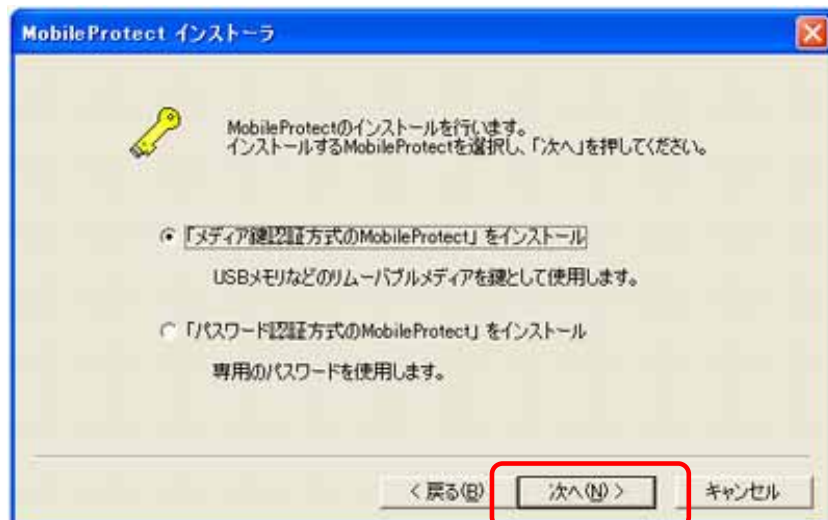
- 新規インストール時　　　¥tools¥環境チェックUTL¥MPEnvChk.EXE
- アップグレードインストール時　　¥tools¥環境チェックUPG¥MPEnvChkUpg.EXE

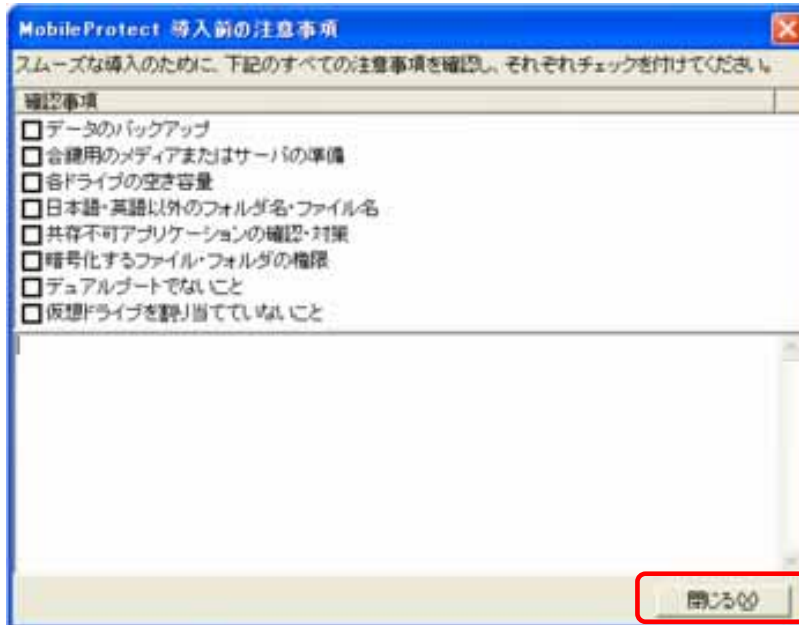
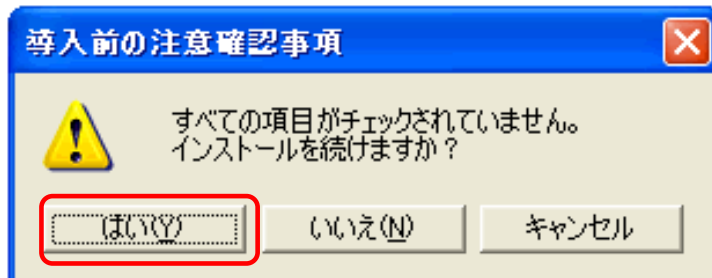
※ CD-ROM からコピーして使用する場合は、¥環境 UTL フォルダをデスクトップなどにコピーしてから実行してください。
（MPEnvChk.EXE は実行ファイルのみをコピーしても動作しません。）

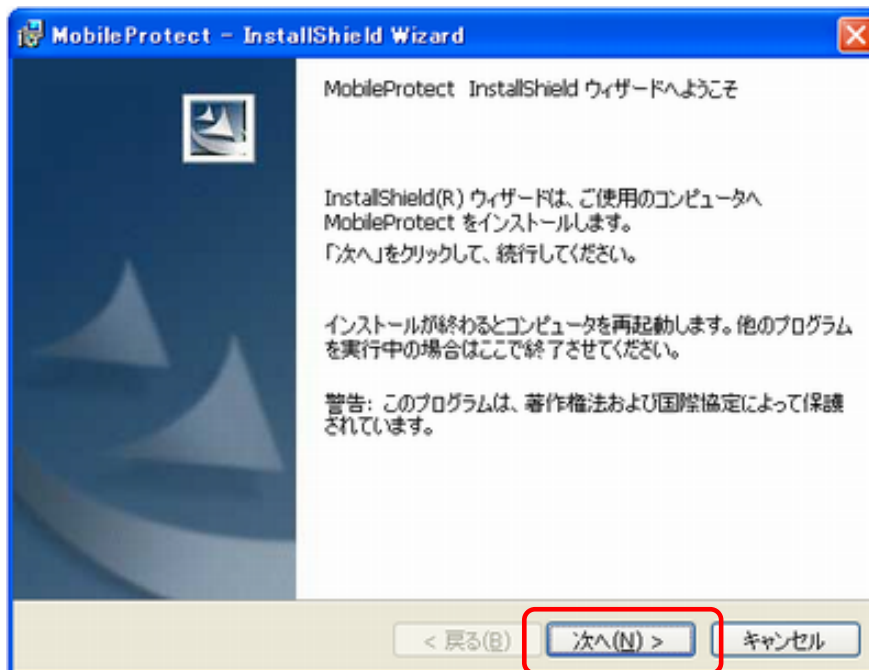
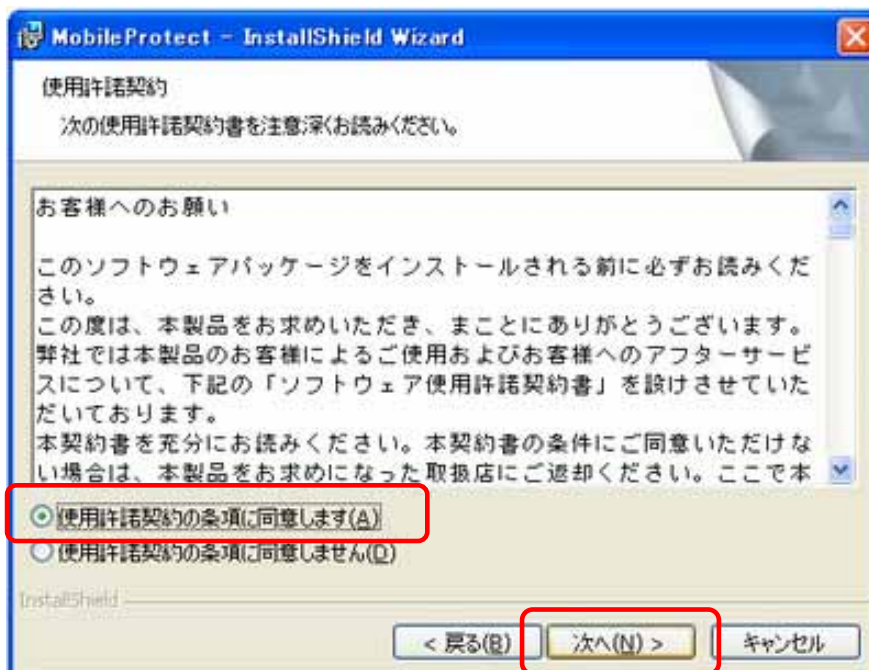
問題が見つかった場合は、すべて対処してください。画面内の「対処方法」をクリックすると、対処方法が表示されます。

（1）　本ソフトウェアが格納されているメディア（例　CD-ROM）内の setup.exe を実行し、「次へ」をクリックしてください。

（2）　『「メディア鍵認証方式の MobileProtect」をインストール』または『「パスワード認証方式の MobileProtect」をインストール』のいずれかを選択し、「次へ」をクリックしてください。

※　管理者によって運用形態が設定されている場合は、この画面は表示されません。

※　アップグレードの場合、「アップグレードインストールを行います」と表示されますので、「次へ」をクリックし、「続行しますか？」と表示されましたら「はい」をクリックしてください。

（3）　「導入前の注意事項」画面が表示されます。各項目をクリックすると詳細な説明が表示されますので、必ずお読みの上、チェックを付けてください。すべての確認が終わりましたら、「閉じる」をクリックしてください。

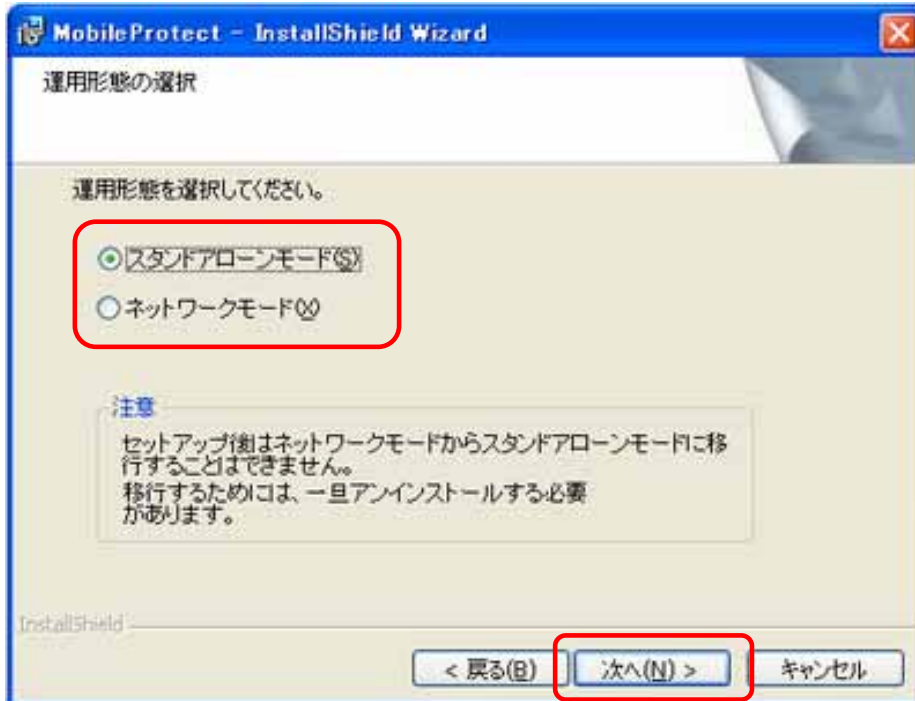
※画面はメディア鍵認証方式の場合です。パスワード認証方式の場合は一部異なります。

（4）　すべての項目がチェックされていない場合は、下記のメッセージが表示されます。
インストールを続ける場合は「はい」を、インストールを中止する場合は「いいえ」を、(3)の画面に戻る場合は「キャンセル」をクリックしてください。

（5）　「次へ」をクリックしてください。

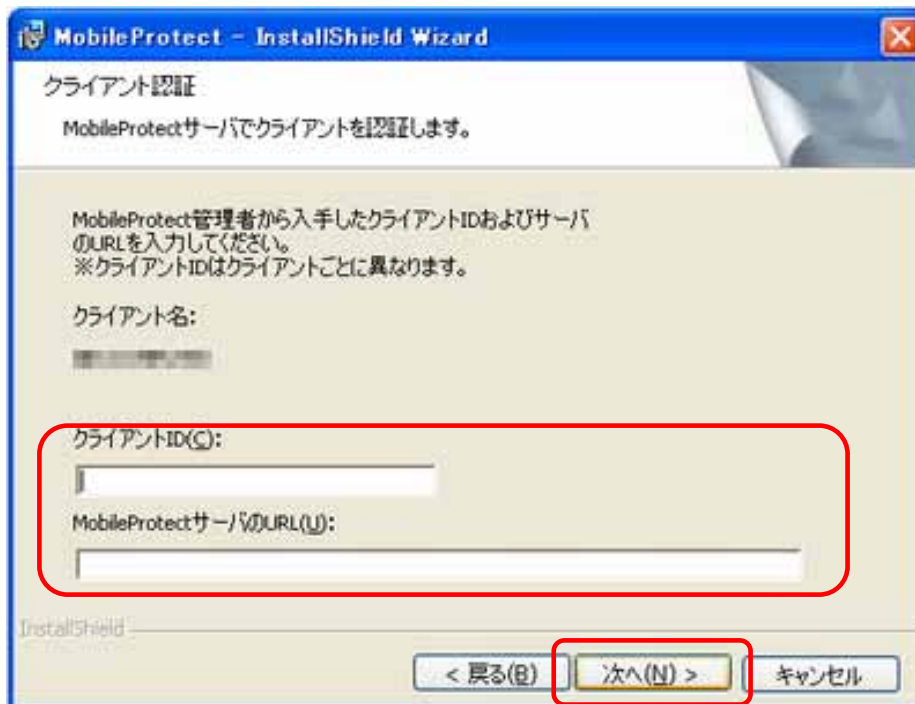
※ アップグレードの場合、お使いのバージョンによっては「MobileProtect 用の InstallShield ウィザードを続行しています」と表示されますので、(8)または(12)へ。

（6）　使用許諾契約をすべてお読みいただき、同意する場合は「使用許諾契約の条項に同意します」をクリックしてください。
「使用許諾契約の条項に同意しません」を選択した場合はインストールできません。

（7）　ユーザ情報を入力します。
【ユーザ名】、【会社名】、【プロダクトID】、【スーパーバイザパスワード／ユーザパスワード】を入力します。
（確認のため、スーパーバイザパスワード／ユーザパスワードは2回入力してください。）
すべての入力が終わりましたら、「次へ」をクリックしてください。

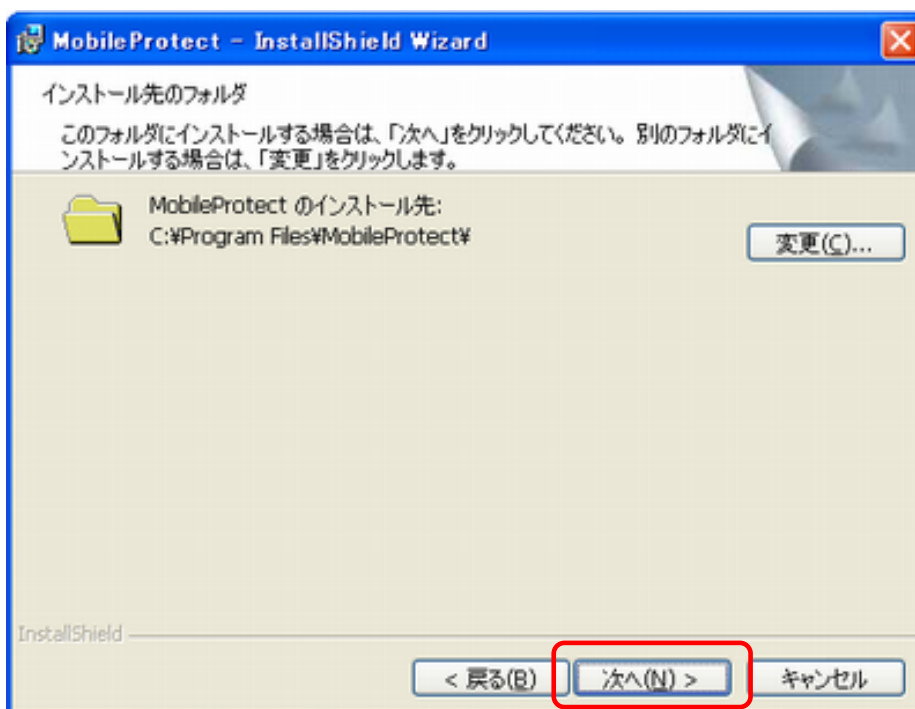
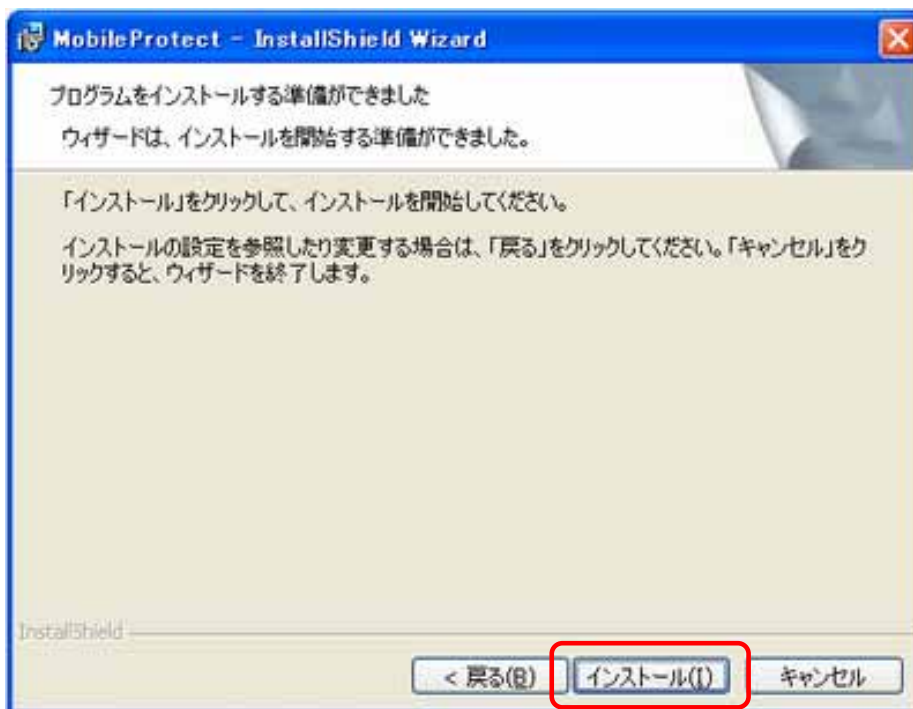
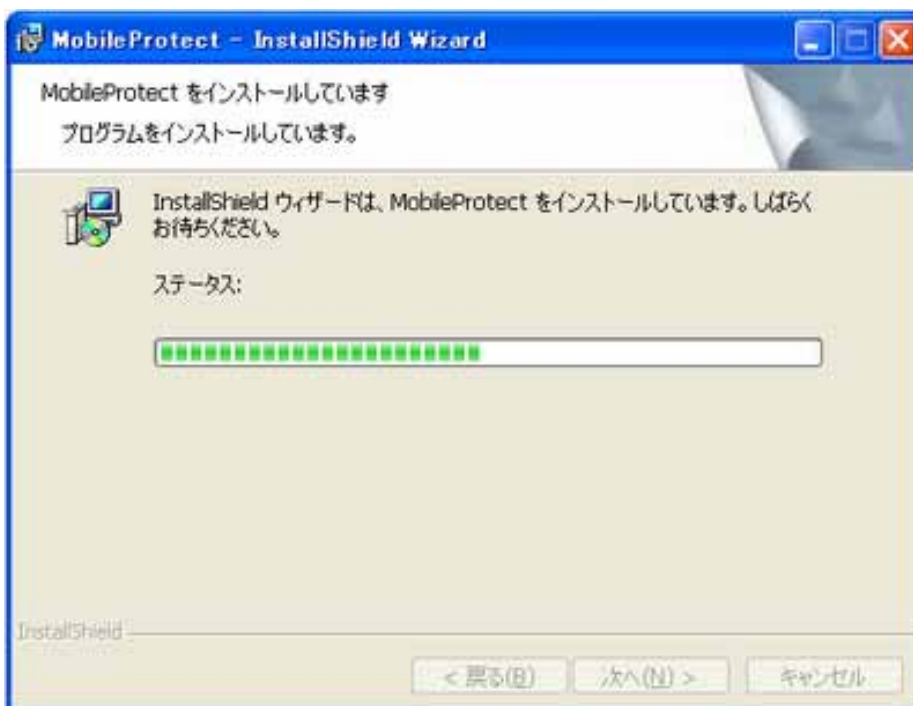
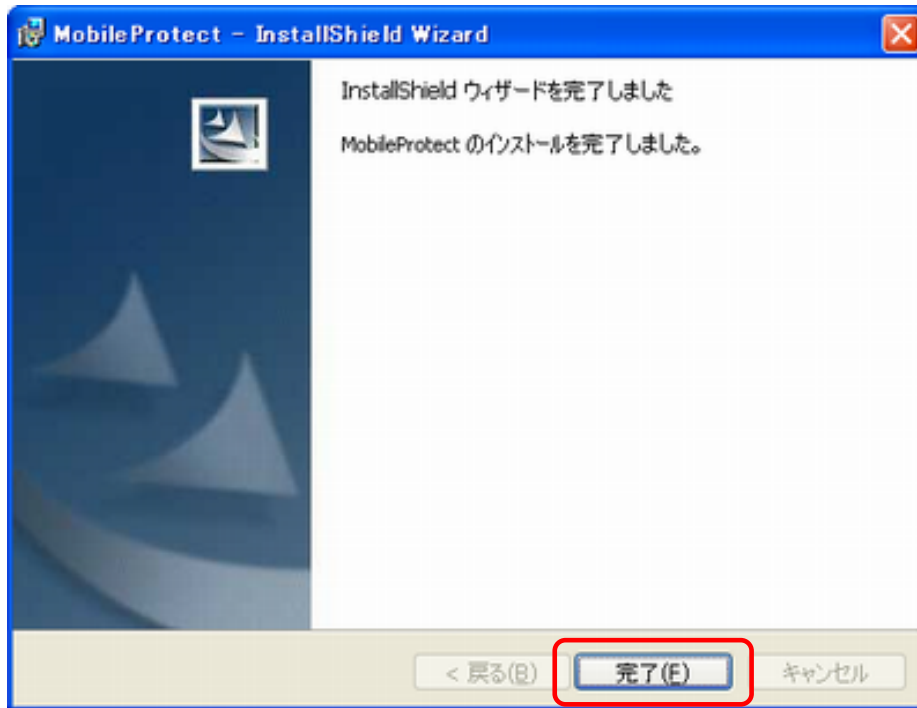
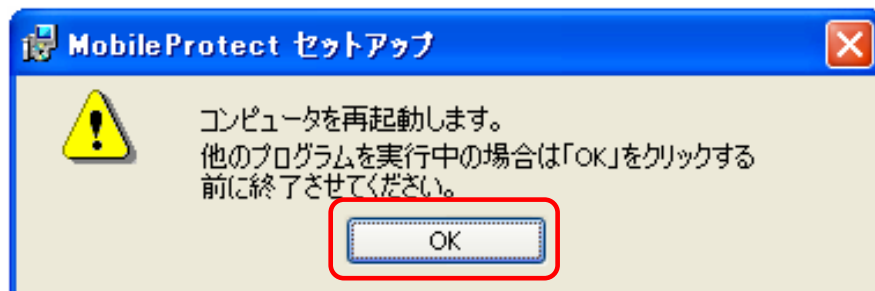
※　ユーザ名、会社名は半角 40 文字以内、または全角 20 文字以内で入力してください。
※　プロダクト ID はユーザ証書に記載されているものを半角文字で入力してください。
（大文字小文字は区別しません）。
※　スーパーバイザパスワードは 8 桁以上 64 桁以内の半角文字を、ユーザパスワードは 8 桁以上 32 桁以内の半角文字を指定してください。
（大文字小文字を区別します）。
※　画面はメディア鍵認証方式版です。パスワード認証方式版の場合は、「スーパーバイザパスワード」の欄は「ユーザパスワード」と表示されます。
※　スーパーバイザパスワード／ユーザパスワードとは【MobileProtect ユーティリティ】を起動するときなどに必要なパスワードですので、忘れないよう注意してください。

(8) 「運用形態の選択」画面で、運用形態の選択をします。

※ 別売の InfoCage/モバイル防御管理サーバが導入されていない環境では、スタンドアローンモードを選択してください。
InfoCage/モバイル防御管理サーバが導入されている環境では、本ソフトウェア管理者に問い合わせて運用形態を選択してください。

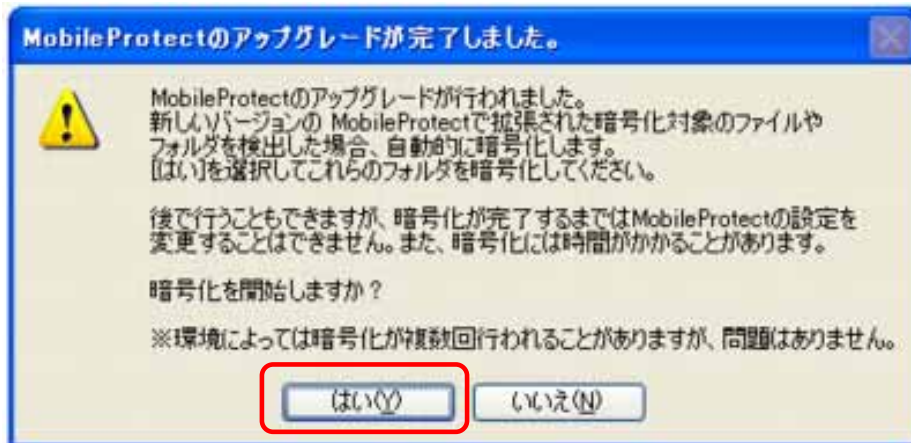
※ 管理者によって運用形態が設定されている場合は、この画面は表示されません。

※ スタンドアローンモードを選択した場合は(10)へ。

（9） ≪ネットワークモード≫を選択した場合、「クライアント認証」画面が表示されるので、【クライアントID】、【MobileProtect サーバ】の URL を入力して、「次へ」をクリックしてください。
※　スタンドアローンモードの場合、この画面は表示されません。
※　管理者によって運用形態が設定されている場合は、この画面は表示されません。

※　認証に失敗をした場合は、【クライアント名】、【クライアント ID】、【MobileProtect サーバの URL】を確認後、管理者に問い合わせてください。
※　管理者がクライアント登録をしていない場合は認証されません。

（10）インストール先のフォルダ選択画面で本ソフトウェアのインストールフォルダを選択します。
通常はそのまま「次へ」をクリックしてください。

（11）「インストール」をクリックしてインストールを開始してください。

（12）インストール中です。しばらくお待ちください。

（13）インストールが完了すると下記の画面が表示されます。「完了」をクリックしてください。

（14）本ソフトウェアを使用可能にするためには、パソコンを再起動する必要があります。他のプログラムを実行中の場合は、終了させてください。
「OK」をクリックすると、パソコンが再起動します。

アップグレードインストールを行った場合

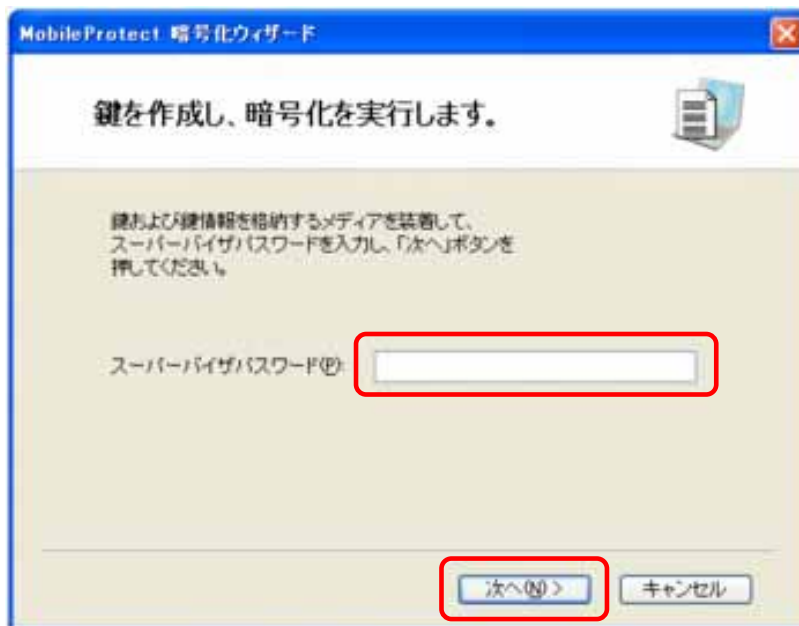
以前のバージョンからアップグレードインストールを行った場合、再起動後に表示されるパスワード入力画面でスーパーバイザパスワード／ユーザパスワードを入力すると、下記のメッセージが表示されます。

※ パスワード認証方式でインストールを行い、セキュリティチップ（TPM）搭載のパソコンをお使いの場合は、セキュリティチップ（TPM）に関するメッセージの後に表示されます。

必ずお読みの上、「はい」をクリックしてください。
暗号化を後で行う場合は「いいえ」をクリックしてください。
「いいえ」をクリックした場合、暗号化が完了するまでは【MobileProtectユーティリティ】を起動するごとにメッセージが表示されます。

※ アップグレードの場合は暗号化が完了したら操作は終了です。

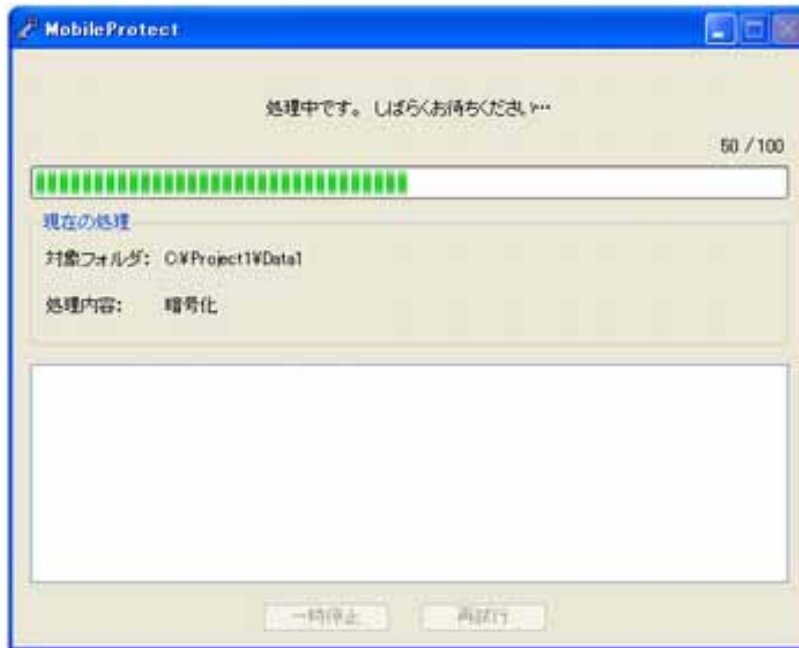
3.2 インストール（Step2）

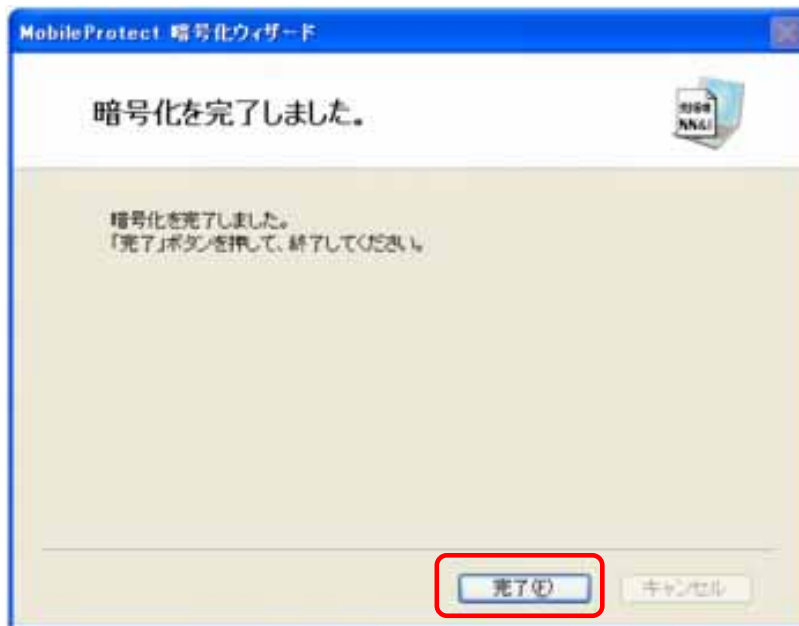
3.2.1 メディア鍵認証方式の場合

（1） 再起動後、下記の画面が表示されます。鍵を格納するメディアと鍵情報を格納するメディアを装着し、インストール時に設定したスーパーバイザパスワードを入力して「次へ」をクリックしてください。

※ 他のパソコンの【MobileProtect ユーティリティ】または【メディア暗号ユーティリティ】で暗号化したリムーバブルメディアは、暗号化を実行する前に必ず抜いてください。装着したまま暗号化を開始すると上図と異なる画面が表示されますので、一旦「キャンセル」をクリックし、リムーバブルメディアを抜いてから再度【MobileProtect ユーティリティ】を起動して操作してください。

（2） 鍵および鍵情報を作成します。
※ 管理者によりあらかじめ鍵および鍵情報の格納先が設定されている場合は下記の画面が異なります。

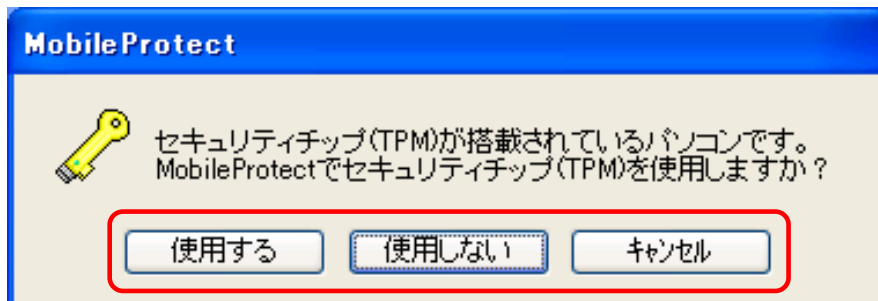
鍵を格納するメディア および 鍵情報を格納するメディアを選択して「次へ」をクリックしてください。格納するメディアが表示されないときは、「更新」をクリックしてください。

※ 暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

（3） 暗号化処理中です。しばらくお待ちください。

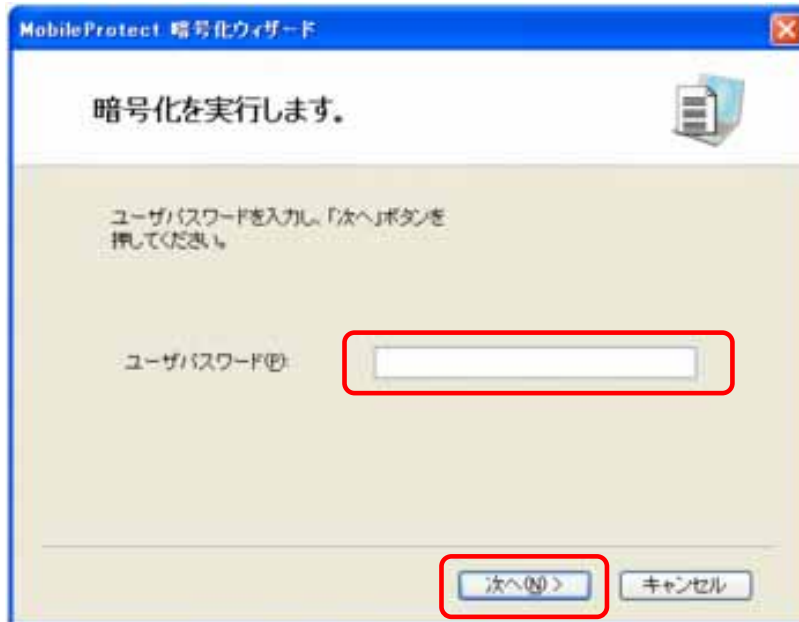
（4） 暗号化を完了しました。「完了」をクリックしてください。

（5） 以上でインストールは完了しました。
その他の設定については、【MobileProtect オンラインマニュアル】を参照してください。

※ この段階では、ProgramFiles やアプリケーションのインストールフォルダ以下は暗号化されていません。ProgramFiles やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、オンラインマニュアルの「MobileProtect ユーティリティ＞暗号化指定」を参照してください。

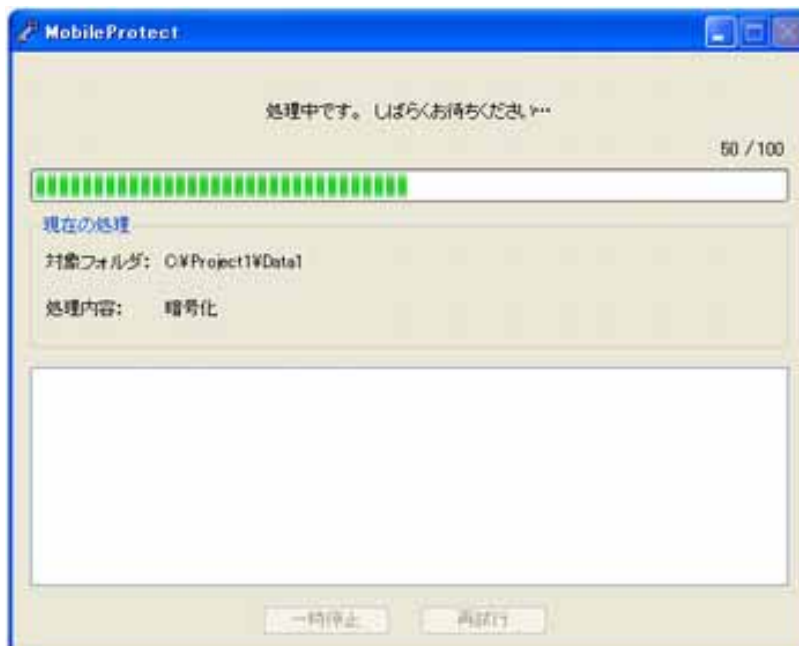
3.2.2　パスワード認証方式の場合

■ セキュリティチップ（TPM）搭載のパソコンをお使いでセキュリティチップ（TPM）が有効になっている場合
再起動後、インストール時に設定した InfoCage/モバイル防御のユーザパスワードを入力して Windows にログオンすると、下記の画面が表示されます。

セキュリティチップ（TPM）を使用する場合は「使用する」を、使用しない場合は「使用しない」を、後で選択する場合は「キャンセル」をクリックしてください。続いて(1)の画面が表示されます。
「キャンセル」をクリックした場合、TPMの使用を選択するまで【MobileProtectユーティリティ】の起動時にメッセージが表示されます。

※　セキュリティチップ（TPM）に関しては、「第5章　セキュリティチップ（TPM）搭載のパソコンをお使いの場合」を参照してください。

（1）再起動後、インストール時に設定した InfoCage/モバイル防御のユーザパスワードを入力して Windows にログオンすると、下記の画面が表示されます。「次へ」をクリックしてください。

※　他のパソコンの【MobileProtect ユーティリティ】またはメディア暗号ユーティリティで暗号化したリムーバブルメディアは、暗号化を実行する前に必ず抜いてください。装着したまま暗号化を開始すると上図と異なる画面が表示されますので、一旦「キャンセル」をクリックし、リムーバブルメディアを抜いてから再度【MobileProtect ユーティリティ】を起動して操作してください。

（2）暗号化を実行します。「次へ」をクリックしてください。

※　暗号化するフォルダ内のファイル数が多い場合、暗号化に時間がかかる場合があります。

（3）　暗号化処理中です。しばらくお待ちください。

（4）　暗号化を完了しました。「完了」をクリックしてください。

（5）　以上でインストールは完了しました。
その他の設定については、【MobileProtect オンラインマニュアル】を参照してください。

※　この段階では、ProgramFiles やアプリケーションのインストールフォルダ以下は暗号化されていません。ProgramFiles やアプリケーションのインストールフォルダ以下にあるデータファイルを個別に暗号化するには、オンラインマニュアルの「MobileProtect ユーティリティ＞暗号化指定」を参照してください。

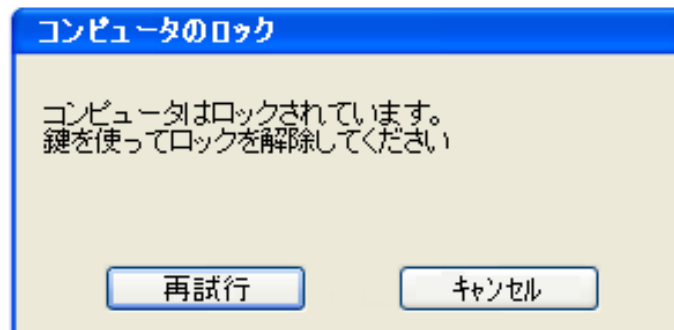
第4章　ログオン方法

4.1　メディア鍵認証方式の場合

（画面イメージは Windows XP　Professional です）

起動しているパソコンから鍵を抜いた場合

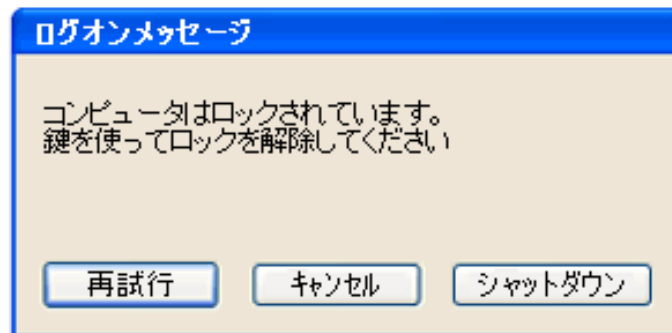
起動しているパソコンから鍵を抜くと、「コンピュータのロック」画面が表示され、パソコンがロックされた状態になります。
※Windows の設定によっては、「コンピュータのロック」画面は表示されない場合があります。

鍵を抜いた状態でログオンしようとすると、「コンピュータはロックされています。鍵を使ってロックを解除してください。」と表示され、ログオンできません。

鍵を装着して「再試行」をクリックすると、「コンピュータのロックの解除」画面が表示され、パスワードを入力するとロックが解除され、ログオンすることができます。

鍵を抜いた状態でパソコンを起動した場合

パソコンを起動すると「Windows へようこそ」画面が表示されます。

※ Windows の設定によっては、「Windows へようこそ」画面は表示されずに「ログオンメッセージ」画面が表示されます。

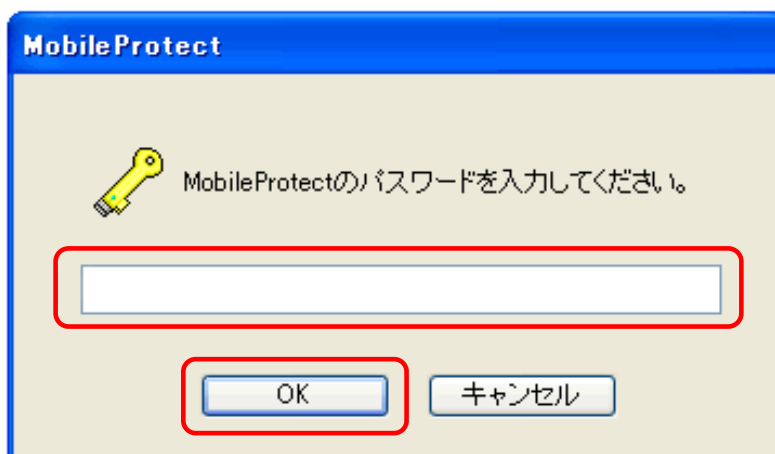
鍵を抜いた状態でログオンしようとすると、「コンピュータはロックされています。鍵を使ってロックを解除してください。」と表示され、ログオンできません。

鍵を装着して「再試行」をクリックすると、「Windows へログオン」画面が表示され、パスワードを入力するとロックが解除され、ログオンすることができます。

4.2　パスワード認証方式の場合

（画面イメージは Windows XP　Professional です）

再起動後に、通常のログオン画面が表示されます。
Ctrl＋Alt＋Del キーを押してください。

※　Windows の設定によっては、「Windows　へようこそ」画面は表示されません。

ユーザパスワード入力画面が表示されます。
インストール時に設定したユーザパスワードを入力し、「OK」をクリックしてください。

※　ユーザパスワードを 5 回誤って入力すると、「OK」がクリックできなくなります。その場合は「シャットダウン」をクリックして一旦シャットダウンした後、しばらくしてから再度パソコンを起動してください。（すぐにパソコンを起動しても一定時間パスワードの入力はできません。）

「Windows へログオン」画面が表示され、ユーザ名とWindows ログオンパスワードを入力するとログオンすることができます。

第5章　セキュリティチップ（TPM）搭載のパソコンをお使いの場合

セキュリティチップ（TPM： Trusted Platform Module）とは、PC プラットフォームにおけるセキュリティ技術の業界団体 TCG（Trusted Computing Group）が策定した仕様に準拠した IC チップで、これを使用することにより、様々なセキュリティ機能を利用することが可能になります。

本ソフトウェアのパスワード認証方式では、セキュリティチップ（TPM）の機能を使用することにより、さらに強固なセキュリティを実現できます。

セキュリティチップ（TPM）の使用について

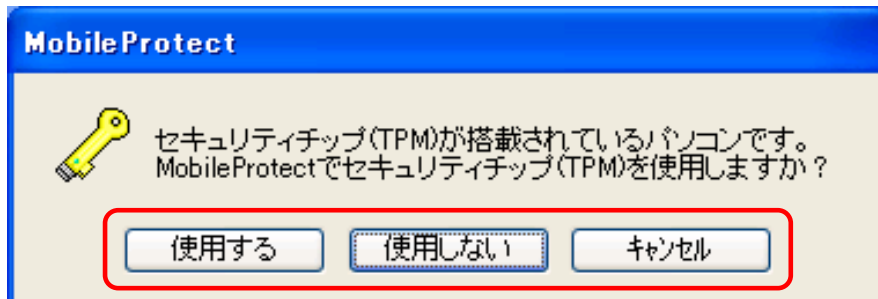
セキュリティチップ（TPM）を有効にした場合は、本ソフトウェアのパスワード認証方式をインストールした場合にセキュリティチップ（TPM）を使用するかを選択することができます。

セキュリティチップ（TPM）を有効にするには、BIOS セットアップでセキュリティチップを「使用する」にし、セキュリティチップユーティリティをインストールしてください。

※ セキュリティチップ（TPM）の設定方法についてはお使いのパソコンのマニュアルを参照してください。

本ソフトウェアのパスワード認証方式をインストール後、【MobileProtect ユーティリティ】の起動時に下記のメッセージが表示されます。

※ 表示されない場合は、管理者にお問い合わせください。

セキュリティチップ（TPM）を使用する場合は「使用する」を、使用しない場合は「使用しない」を、後で選択する場合は「キャンセル」をクリックしてください。
「キャンセル」をクリックした場合、TPMの使用を選択するまで【MobileProtectユーティリティ】の起動時にメッセージが表示されます。

注意事項

- セキュリティチップ（TPM）を使用するには、本ソフトウェアのパスワード認証方式をインストールする前にセキュリティチップ用ドライバおよびユーティリティがインストールされている必要があります。
- BIOS のアップデートなどで設定値を初期化した場合、アップデート後にセキュリティチップの値を必ず元に戻してください。
- セキュリティチップ（TPM）を使用している場合、セキュリティチップユーティリティをアンインストールしないでください。アンインストールすると暗号化されたファイルにアクセスできなくなります。
- セキュリティチップ（TPM）を使用している場合、BIOS でセキュリティチップを「使用しない」に設定を変更したり、設定値の初期化をしたりすることは絶対にしないでください。これらの操作を実行した場合、暗号化されたファイルにアクセスできなくなります。

第６章 ユーティリティの起動及び、オンラインマニュアルの参照方法

●【MobileProtect ユーティリティ】を起動するには

スタートメニューから、［すべてのプログラム］－［MobileProtect］－［MobileProtect ユーティリティ］をクリックしてください。

●【MobileProtect オンラインマニュアル】を参照するには

スタートメニューから、［すべてのプログラム］－［MobileProtect］－［MobileProtect オンラインマニュアル］をクリックしてください。

第7章 初期暗号化モードの設定

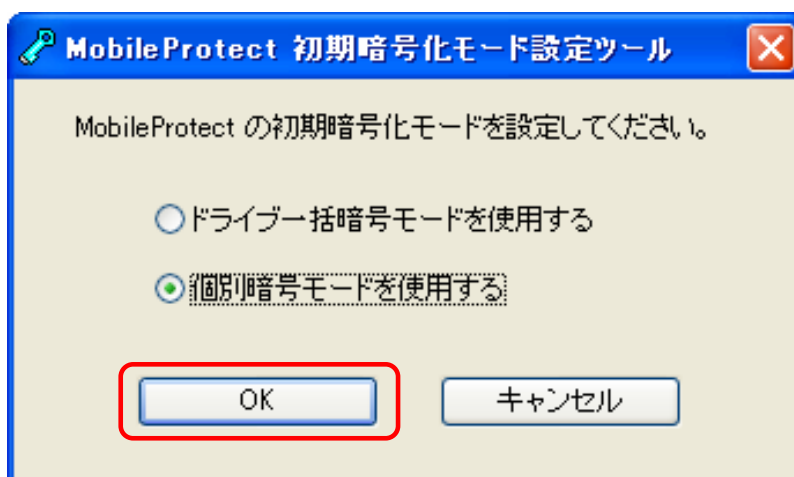
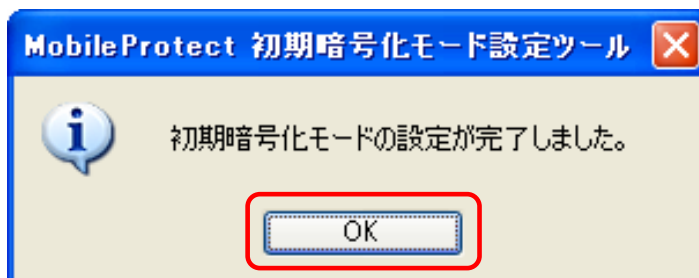
本ソフトウェアは、下記の 2 通りのモードでインストールを行うことができます。

- ドライブ一括暗号モード（既定の導入モード）
  本ソフトウェアが推奨する設定でインストールを行います。本モードでインストールを行う場合は、以下の設定は不要です。
- 個別暗号モード
  暗号化するドライブやフォルダを個別に指定して運用するときは、個別暗号モード用のインストールモジュールを作成してインストールを行います。

※ 初期暗号化モードを設定せずにインストールを行うと、「ドライブ一括暗号モード」でインストールされます。

初期暗号化モードの設定方法

（1） 本ソフトウェアのクライアント CD-ROM のすべての内容をコンピュータの適当なフォルダにコピーし、メディア鍵認証方式をインストールする場合は¥MP フォルダ内の、パスワード認証方式をインストールする場合は¥MP_PW¥フォルダ内の MPSetWiz.exe を実行してください。

（2） 初期暗号化モードを選択して「OK」をクリックしてください。

（3） 設定が完了しました。「OK」をクリックしてください。

（4） 初期暗号化モードを設定したセットアッププログラムが作成されましたので、CD-ROM 内の「個別暗号モードインストールガイド.PDF」にしたがってインストールしてください。

第8章 トラブルシューティング

インストール時に「1607:InstallShield Scripting Runtime をインストールできません。」というメッセージが表示され、インストールできない。

このエラーは、InstallShield が次のような原因で正常に動作していないときに表示されます。

(1)　管理者権限の無いユーザでログオンしている。
- インストールする際のユーザ権限は、コンピュータの管理者（アドミニストレータ権限）で行ってください。

(2)　IDriver.exe が正しく登録されていない。
- Windows のコマンドプロンプトから以下のコマンドを実行して、IDriver.exe を登録しなおしてください。
¥ProgramFiles¥CommonFiles¥InstallShield¥Driver¥7¥Intel32¥IDriver.exe/REGSERVER （注1）

※ Windows が C ドライブにインストールされている場合の例です。それ以外のドライブにインストールされている場合には、該当するドライブ文字に置き換えてください。
※ （注1）下線部はお使いの環境によって異なる場合があります。

(3)　同時に複数のインストーラが起動している。
- 誤って Setup.exe を複数実行してしまった場合、一旦全てのインストーラを終了してから、再度インストールを行ってください。

(4)　Windows インストーラ(msiexec.exe)が正しく登録されていない。
- 任意の場所（デスクトップ等）に[新規作成]でテキストファイルを作成し、ファイルの拡張子を.txt から.msi に変更してください。
アイコンがインストーラのアイコンに変わるか確認します。
アイコンがインストーラのアイコンに変わらない場合は、コマンドプロンプトで以下のコマンドを実行してください。
C:¥Windows¥System32¥msiexec.exe /REGSERVER

※ WindowsXP が C ドライブにインストールされている場合の例です。
それ以外のドライブにインストールされている場合には、該当するドライブ文字に置き換えてください。
また、OS が異なる場合はシステムフォルダ名を置き換えてください。

(5)　Windows XP で、「SUBST」コマンドで作成した仮想ドライブからインストールを実行している。
SUBST コマンドによる仮想ドライブを解除してください。

※その他についてはオンラインマニュアルのトラブルシューティングをご参照ください。